

Ciberseguridad para Padres

Una guía práctica para proteger a tu familia
en el mundo digital



Jorge Kero

Índice

Capítulo 1. Introducción a la Ciberseguridad: ¿Por qué es importante para padres?	7
Capítulo 2. Contraseñas y Seguridad Básica	11
Capítulo 3. Protección contra Fraudes y Estafas Digitales	15
Capítulo 4. Control Parental y Protección de Menores	19
Capítulo 5. Redes Sociales – Riesgos y Buenas Prácticas	23
Capítulo 6. Seguridad en Dispositivos y Redes del Hogar	27
Capítulo 7. Herramientas Útiles para Padres Digitales	31
Capítulo 8. Cómo actuar ante un incidente (fraude, acoso, acceso no autorizado)	35
Capítulo 9. Hacia una cultura digital familiar	39
Capítulo 10. Videojuegos, tiempo en pantalla y adicción digital	43
Capítulo 11. Inteligencia artificial y niños: asistentes, apps y voz	47
Capítulo 12. Privacidad de los padres: lo que también debemos proteger	51
Capítulo 13. Herramientas para educar digitalmente en el aula y en casa	55
Capítulo 14. Cómo gestionar los conflictos digitales en casa	59
Conclusión: Educar en el mundo digital también es amar con responsabilidad	63

Este libro ha sido escrito por Jorge Kero, apoyado por la plataforma de ChatGPT, para su estructuración e inclusión adicional de material, como las ilustraciones. Creado en junio de 2025.

Capítulo 1: Introducción a la Ciberseguridad: ¿Por qué es importante para padres?

Cuando hablamos de ciberseguridad, nos referimos a las medidas, hábitos y herramientas que usamos para proteger nuestros dispositivos (teléfonos móviles, ordenadores, tabletas) y, especialmente, nuestra información personal cuando estamos conectados a internet. Es la práctica que nos ayuda a evitar riesgos digitales como robos de identidad, fraudes financieros, virus informáticos, acoso en línea o invasiones a la privacidad.

Para muchos padres, la palabra “ciberseguridad” puede parecer técnica, confusa o incluso lejana. Es común pensar que estas cosas les suceden a otros, pero la realidad es que la mayoría de las personas estamos expuestas diariamente a riesgos digitales, especialmente quienes tienen hijos menores de edad en casa, puesto que los niños y adolescentes son particularmente vulnerables en este entorno.

No es necesario ser un experto en tecnología para entender los conceptos básicos y adoptar prácticas sencillas que marquen una gran diferencia en la protección de tu familia.



¿Por qué la ciberseguridad debería preocupar especialmente a los padres?

La razón principal es que, como padre o madre, tu tarea primordial es garantizar la seguridad física y emocional de tus hijos. En la actualidad, esta tarea también se extiende al mundo digital. Tus hijos nacieron en un entorno tecnológico, donde las redes sociales, juegos online y aplicaciones móviles son parte integral de su vida diaria.

Este acceso constante a internet les brinda enormes ventajas educativas y sociales, pero también los expone a peligros que probablemente tú no enfrentaste a su edad. Algunos ejemplos de estos riesgos incluyen:

- **Ciberacoso:** insultos, amenazas o burlas constantes a través de redes sociales.
- **Contenido inapropiado:** material violento o adulto que podría afectar emocionalmente a tus hijos.
- **Robo de identidad:** estafadores que utilizan información personal para cometer fraudes.

- **Estafas online:** ofertas falsas, sorteos fraudulentos, o mensajes de phishing (correos o mensajes diseñados para engañar y obtener datos personales).

La seguridad digital no es solo una cuestión técnica; es una responsabilidad parental moderna, tan vital como enseñarles seguridad vial o la importancia de no hablar con desconocidos.

Riesgos frecuentes que padres deben conocer

Los riesgos más habituales en internet y dispositivos digitales son los siguientes:

- **Phishing (suplantación de identidad):** mensajes falsos enviados por correo o WhatsApp que intentan convencerte de que reveles datos privados o financieros. Estos mensajes pueden parecer legítimos, como un supuesto aviso bancario o de una agencia tributaria.
- **Malware (software malicioso):** virus, gusanos o programas espía que infectan tu dispositivo para robar información o dañarlo. Muchas veces vienen ocultos en aplicaciones aparentemente inocentes o en enlaces que reciben tus hijos en chats o redes sociales.
- **Ciberacoso (bullying digital):** el acoso tradicional trasladado a entornos digitales, donde el daño emocional puede ser igual o más intenso debido a su persistencia y alcance.
- **Robo de identidad:** los delincuentes usan datos personales obtenidos en redes sociales o dispositivos comprometidos para realizar compras, préstamos o incluso cometer delitos bajo el nombre de alguien más.
- **Grooming:** adultos que, escondiendo su identidad, se acercan a menores a través de juegos online o redes sociales, buscando explotarlos sexualmente o manipularlos emocionalmente.

Conocer estos riesgos es fundamental porque te permite anticiparte y prevenir posibles problemas antes de que ocurran.

Impacto emocional y económico de la falta de seguridad digital

La falta de ciberseguridad puede causar efectos devastadores para una familia. Económicamente, puedes enfrentar fraudes o robos que signifiquen pérdidas monetarias significativas. Por ejemplo, si alguien accede ilegalmente a tus cuentas bancarias, podría vaciarlas en minutos.

Emocionalmente, las consecuencias son aún más preocupantes. El acoso digital o grooming pueden causar ansiedad, estrés, depresión e incluso tener consecuencias aún más graves en la salud mental de tus hijos. Además, la invasión de la privacidad puede hacer que una persona se sienta vulnerable y violada en su espacio personal.

Como padre o madre, la prevención y una comunicación clara sobre seguridad digital son tus mejores herramientas para evitar estos impactos negativos.

La importancia del ejemplo: los padres como modelos digitales

Los niños aprenden por imitación. Tu actitud y comportamiento respecto a la tecnología marcarán la pauta para ellos. Si usas contraseñas débiles, compartes tu información personal fácilmente o no

muestras preocupación sobre quién tiene acceso a tus datos, tus hijos lo percibirán como algo normal y aceptable.

Por el contrario, si adoptas hábitos seguros como mantener contraseñas robustas, revisar configuraciones de privacidad en redes sociales, y usar antivirus o aplicaciones de protección parental, enseñarás con el ejemplo, dejando claro que la seguridad digital es algo valioso y necesario.

Incluso más importante, al fomentar una comunicación abierta sobre los riesgos en línea y sobre cómo enfrentarlos juntos, ayudas a generar confianza y seguridad emocional en tus hijos. Así, ellos acudirán a ti si algo preocupante sucede en línea.



¿Qué puedes esperar del resto del libro?

A lo largo de los próximos capítulos, aprenderás de manera sencilla y clara cómo implementar prácticas efectivas y realistas para mejorar la seguridad digital en tu hogar. Veremos cómo proteger la información personal, usar herramientas prácticas como controles parentales, reconocer posibles amenazas en línea, hablar claramente con tus hijos sobre los peligros digitales, y mucho más.

Cada capítulo incluirá ejemplos claros y casos prácticos que te permitirán comprender fácilmente cómo aplicar estos conceptos en tu vida diaria.



Resumen de este capítulo:

- La ciberseguridad protege tus dispositivos e información personal de amenazas digitales.
- Padres deben preocuparse especialmente por la seguridad digital de sus hijos debido a su vulnerabilidad en internet.
- Los principales riesgos incluyen phishing, malware, ciberacoso, robo de identidad y grooming.
- La inseguridad digital puede causar daños económicos graves y serias consecuencias emocionales.
- Dar un buen ejemplo digital y mantener una comunicación abierta son clave para proteger a tu familia.



¿Qué sigue?

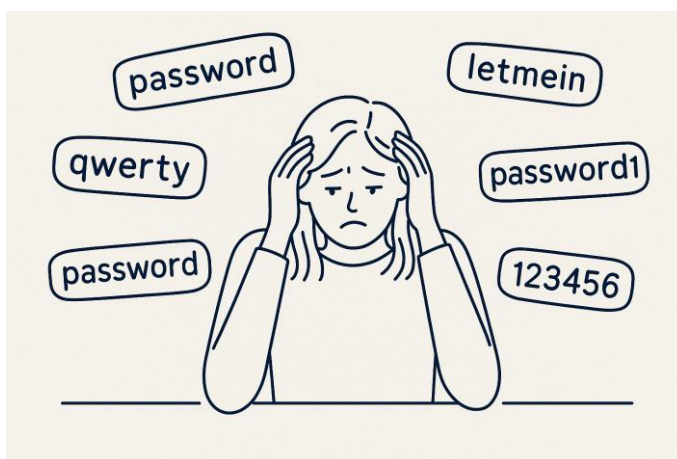
En el próximo capítulo hablaremos sobre **“Contraseñas y Seguridad Básica”**, donde aprenderás cómo crear contraseñas seguras y proteger fácilmente tu vida digital.

Capítulo 2: Contraseñas y Seguridad Básica

? ¿Por qué preocuparse tanto por las contraseñas?

Si te preguntara qué tienen en común tu cuenta bancaria, tu correo electrónico y las redes sociales, ¿qué dirías? Todas dependen de una contraseña para proteger tu información personal y tus recursos económicos. Aun así, muchas personas todavía usan contraseñas como “123456”, “qwerty”, o incluso su fecha de nacimiento.

La razón por la que insistimos tanto en crear contraseñas fuertes es simple: la mayoría de los ataques en línea se producen por contraseñas débiles. Un delincuente digital o hacker puede usar herramientas automáticas capaces de probar millones de combinaciones hasta encontrar la tuya. Es cuestión de minutos o incluso segundos si tu contraseña es demasiado sencilla.



🔒 Qué hace a una contraseña realmente segura

Una contraseña robusta debe cumplir varias condiciones:

- **Longitud:** al menos 12 caracteres.
- **Diversidad de caracteres:** combinar mayúsculas, minúsculas, números y símbolos especiales (como @, !, &, %, \$).
- **Sin datos personales evidentes:** no uses nombres, fechas de cumpleaños o aniversarios, ni nombres de mascotas.
- **Única por cada cuenta importante:** no repitas contraseñas.

Una contraseña que cumpla con estas reglas sería difícil de adivinar incluso para programas informáticos avanzados.

🔒 Métodos efectivos para crear contraseñas fáciles de recordar pero seguras

1. Método de la frase memorable (ampliado)

Escoge una frase significativa para ti, pero que nadie más pueda adivinar fácilmente. Por ejemplo:

Frase: “Me gusta caminar con mis hijos Juan y María los domingos”.

Extrae la primera letra de cada palabra:

mgccmhJyMld

Ahora sustituye algunas letras por números o símbolos parecidos:

- E → 3
- A → @
- I → 1
- → 0

La frase transformada podría ser:

mgccmhJyMld → mgccmhJyMld → mgccmhJyMld → mgccmhJyMld → mgccmhJyMld

Aplicando cambios simples (por ejemplo la “a” de “caminar” o la “i” de “mis”) queda así:

mgccmhJyMld → mgccmhJyMld → mgccmhJyMld → mgccmhJyMld → mgccmhJyMld

Resultado final fácil y fuerte:

mgccmhJyMld → mgccmhJyMld → mgccmhJyMld → mgccmhJyMld → mgccmhJyMld

2. Método de palabras aleatorias

Si prefieres algo más fácil visualmente, usa 3 o 4 palabras sin relación entre ellas, separadas por guiones o puntos. Ejemplo:

- **Mesa-Nube-Piña-Silla**
- **Avión.Tigre.Luna.Gafas**

Añade algún número o símbolo y tendrás una contraseña muy segura:

- **Mesa-Nube-Piña-Silla23**
- **Avión.Tigre.Luna.Gafas!**

Estos métodos son muy fáciles de recordar porque evocan imágenes claras.



Cómo gestionar múltiples contraseñas de manera sencilla y segura

Si tienes cuentas en muchas plataformas (correo electrónico, bancos, tiendas online, redes sociales), probablemente te resulte complicado recordar todas tus contraseñas, especialmente si sigues las recomendaciones y son todas únicas. Aquí es donde entran los **gestores de contraseñas**.



Gestores de contraseñas explicados a fondo

Un gestor de contraseñas es una aplicación que almacena todas tus contraseñas encriptadas en un solo lugar seguro. Solo tienes que recordar una única contraseña maestra para acceder a todas ellas.

Ventajas prácticas de usar gestores de contraseñas:

- **Mayor seguridad:** generas contraseñas automáticas extremadamente fuertes.
- **Comodidad:** la aplicación rellena automáticamente los formularios de login.
- **Sin necesidad de recordar múltiples claves:** solo memorizas una clave fuerte principal.

Ejemplos y recomendaciones:

- **LastPass:** Muy sencillo y popular, fácil de instalar en navegador y móvil.
- **Bitwarden:** Código abierto y completamente seguro, gratuito en versión básica.
- **Dashlane:** Excelentes funciones de seguridad adicional (alertas de violaciones).



Autenticación en dos pasos (2FA): protección adicional indispensable

La **autenticación en dos pasos (2FA)** protege tus cuentas exigiendo dos factores distintos de identificación:

- **Algo que sabes:** tu contraseña.
- **Algo que tienes:** tu teléfono móvil (recibiendo un código SMS o desde una aplicación autenticadora como Google Authenticator).

Incluso si alguien tiene tu contraseña, no podrá acceder a tu cuenta sin este segundo factor. Esto reduce drásticamente el riesgo de intrusión.



Cómo activarlo en tus cuentas importantes (paso a paso):

1. Inicia sesión en la cuenta (Google, Facebook, Amazon, etc.).
2. Entra en la configuración de seguridad o privacidad.
3. Busca la opción “Verificación en dos pasos” o “Autenticación en dos factores”.
4. Sigue las instrucciones para vincular tu teléfono.
5. Recibirás un código único por SMS cada vez que ingreses.

Esto se realiza una sola vez, y mejora significativamente tu seguridad digital.



Errores más comunes con las contraseñas (y cómo evitarlos)

Muchos usuarios cometen errores graves que les exponen a riesgos:

- **Usar la misma contraseña en todas partes:**
¡No lo hagas! Si alguien roba tu contraseña de Facebook, podría acceder a tu banco o email.
- **Cambiar contraseñas periódicamente (pero a una más débil):**
Cambia solo si tienes sospecha de compromiso o periódicamente por otra robusta y diferente.
- **Compartir contraseñas por mensajes o emails:**
Nunca envíes contraseñas por estos medios, ya que podrían interceptarse fácilmente.
- **Guardar contraseñas en lugares visibles o documentos no cifrados:**
Usa gestores o libretas seguras en casa.

Ejemplos prácticos ampliados:

- **Cuenta bancaria familiar:** Crea una contraseña robusta con el método de la frase memorable. Activa obligatoriamente 2FA en tu banco.
- **Redes sociales adolescentes:** Enséñales a tus hijos a usar contraseñas únicas para sus perfiles y activar 2FA.
- **Contraseñas del colegio:** Utiliza un gestor familiar para almacenar accesos a plataformas escolares. Enséñale a tus hijos cómo acceder y usar la app.
- **Email personal:** Actualiza inmediatamente tu contraseña a una robusta y diferente, activando 2FA.

**Consejos rápidos para reforzar hoy mismo tu seguridad digital familiar:**

- Crea hoy mismo tu contraseña principal con alguno de los métodos descritos.
- Descarga y comienza a utilizar un gestor de contraseñas.
- Activa 2FA en tus cuentas más importantes inmediatamente.
- Realiza un cambio gradual de contraseñas débiles que tengas guardadas actualmente.

Resumen rápido del capítulo:

- Las contraseñas robustas son esenciales para proteger tus cuentas online.
- Usa frases fáciles de recordar para crear contraseñas seguras.
- Los gestores de contraseñas facilitan la administración de múltiples cuentas y contraseñas.
- La autenticación en dos pasos (2FA) añade una capa extra de seguridad a tus cuentas.
- Evita errores comunes como usar contraseñas repetidas, fáciles de adivinar o escribirlas en lugares inseguros.
- Aplica estos consejos a tus cuentas clave para mejorar la seguridad digital familiar.

En el próximo capítulo: Exploraremos en detalle cómo identificar y protegerse contra fraudes y estafas digitales frecuentes que afectan especialmente a familias.

Capítulo 3: Protección contra Fraudes y Estafas Digitales

Introducción: ¿Por qué debemos estar tan atentos?

Vivimos conectados: compramos, hablamos, trabajamos, estudiamos y socializamos a través de una pantalla. Y aunque esta conexión nos ofrece enormes ventajas, también abre una puerta por donde pueden colarse los estafadores digitales. A diferencia de los ladrones tradicionales, los ciberdelincuentes no necesitan romper una cerradura. Solo necesitan que hagas clic.

Para los padres, el reto es doble. No solo debemos protegernos nosotros, sino también enseñar a nuestros hijos —quienes muchas veces son incluso más vulnerables— a defenderse en un mundo digital donde las trampas están por todas partes. Muchas estafas digitales **no parecen peligrosas** al principio. Es justo eso lo que las hace tan efectivas.

¿Qué es exactamente una estafa digital?

Una estafa digital es un intento de engaño a través de medios electrónicos (email, redes sociales, SMS, páginas web falsas, etc.) cuyo objetivo es obtener:

- Datos personales o bancarios.
- Acceso a tus cuentas o dispositivos.
- Dinero, directa o indirectamente.

Los estafadores **usan la tecnología y la psicología**: te engañan apelando a tu confianza, urgencia o miedo. Y lo hacen de forma automatizada, enviando miles de mensajes o creando decenas de webs falsas. Solo necesitan que una mínima parte de las personas caiga.

Tipos de fraudes digitales: conoce al enemigo



Phishing (Correo electrónico falso)

Es, quizá, la estafa digital más extendida. Consiste en enviar correos electrónicos que parecen venir de una entidad conocida (tu banco, Correos, Amazon, PayPal, etc.) para robar tu información personal.

Ejemplo real:

Asunto: "Su cuenta ha sido bloqueada. Haga clic aquí para reactivarla."

Ese enlace no te lleva a tu banco real, sino a una imitación muy bien diseñada.



Consejo práctico: Nunca accedas a tus cuentas desde enlaces de correos. Entra tú mismo escribiendo la dirección real en el navegador.



Smishing (Estafa por SMS o WhatsApp)

Este tipo de fraude llega a tu móvil. Te mandan un SMS urgente diciendo, por ejemplo, que tienes un paquete pendiente de entrega, o que tu cuenta de banco ha sido bloqueada.

Ejemplo real:

"Tu paquete está retenido en aduanas. Haz clic aquí para pagar 2,99€ y liberarlo."

Al hacer clic, pueden pedirte tu tarjeta... y luego vaciarla.



Consejo práctico: Desconfía de cualquier mensaje no solicitado que te pida datos o pagos pequeños.

**Vishing (Llamadas falsas)**

Aquí el engaño ocurre por teléfono. Una voz muy educada te llama fingiendo ser de tu banco, la Seguridad Social o una empresa de confianza. Te piden confirmar datos "por seguridad". A veces tienen tu nombre y DNI, lo cual hace el engaño más creíble.



Consejo práctico: Si no esperas esa llamada, cuelga. Luego, llama tú mismo al número oficial de la entidad en cuestión para comprobar si era cierto.

**Tiendas falsas y productos fantasma**

Muchos anuncios en redes sociales te ofrecen productos de moda, gadgets, zapatillas de marca o ropa a precios sospechosamente bajos. Haces la compra, pagas... y nunca llega nada. O te llega algo completamente distinto.

Señales de alerta:

- No tiene opiniones verificadas.
- Tiene errores de ortografía o frases mal traducidas.
- No aparece una dirección física ni teléfono de contacto.



Consejo práctico: Busca reseñas externas. Copia el nombre de la tienda en Google y añade "estafa" o "opiniones".

**Fraude del "amigo en apuros"**

Un contacto tuyo (amigo, familiar, conocido) te escribe por redes sociales o email pidiendo dinero urgente. Puede decir que está de viaje, sin acceso a su cuenta, o con una emergencia médica.

Pero ese amigo ha sido hackeado. El mensaje no lo envió él.



Consejo práctico: Nunca transfieras dinero por un mensaje. Llama a esa persona antes de hacer nada.

Otras estafas en aumento que debes conocer**Inversiones milagrosas**

Anuncios que te prometen duplicar tu dinero en una semana, ganar con criptomonedas sin experiencia, o invertir con famosos (usando su imagen sin permiso).

 Consejo: No inviertas dinero en ninguna plataforma sin investigar. Verifica si está regulada y nunca des datos bancarios a través de enlaces.

Estafas dirigidas a niños y adolescentes

En juegos online, a veces se ofrecen premios, monedas o “ventajas” a cambio de introducir datos. Los menores pueden no distinguir lo real de lo falso y acabar comprometiendo datos tuyos o suyos.

 Consejo: Usa controles parentales. Habla con ellos sobre no introducir datos ni aceptar nada sin consultarte.

¿Cómo detectar una estafa a tiempo?

Aquí tienes una tabla para imprimir o recordar:

Señal de alerta	Significado
Urgencia artificial	"Actúa ya o perderás tu cuenta"
Remitente extraño	Correos con dominios raros (ej. @cuenta.com.security en lugar de @paypal.com)
Enlace sospechoso	No lleva a la web original. (p. ej. paypal-verif1cacion.com)
Solicita información sensible	Bancos nunca piden contraseñas por email
Promesa exagerada	"Gana 1.000€/día desde casa"
Ortografía dudosa	Muchos errores o lenguaje extraño

¿Qué hacer si tú o tus hijos caen en una estafa?

1. **Cambia las contraseñas inmediatamente.**
2. **Contacta con tu banco** si diste datos financieros.
3. **Activa la autenticación en dos pasos** si aún no lo has hecho.
4. **Denuncia:** Puedes reportarlo en la Oficina de Seguridad del Internauta (OSI) o presentar una denuncia formal en la policía.
5. **Informa a tus contactos** si sospechas que tu cuenta fue comprometida.

No te avergüences. Todos somos vulnerables. Lo importante es actuar rápido.

Educar desde casa: cómo hablar del tema con tus hijos

La mejor defensa es la **prevención**, y eso empieza en casa. Habla del tema con naturalidad. Aquí tienes ideas prácticas para hacerlo:

- **Simula fraudes juntos:** Enséñales mensajes falsos y analícenlos juntos. Puedes buscar capturas reales en la web de la OSI.

- **Repite frases clave:** “Ningún banco te pedirá tu contraseña por email”; “Si no lo esperabas, desconfía”.
- **Juega al detective digital:** Pregúntales si un mensaje es verdadero o falso y por qué.
- **Establece normas claras:** No compartir datos sin tu permiso, no descargar apps sin tu revisión, y no hacer clic en enlaces que reciban sin verificar.

Recursos útiles para proteger a tu familia

- **www.osi.es** – Oficina de Seguridad del Internauta (España).
- **INCIBE** – Instituto Nacional de Ciberseguridad.
- **HavelBeenPwned.com** – Para verificar si tu correo ha sido filtrado en alguna filtración de datos.
- **Antivirus con control parental**, como Norton Family, Qustodio, o Bitdefender.

Resumen del capítulo:

- Las estafas digitales son frecuentes, sutiles y evolucionan constantemente.
- Padres e hijos deben aprender a reconocer señales: urgencia, errores, promesas demasiado buenas.
- Existen muchos tipos: phishing, smishing, tiendas falsas, fraudes de inversión y más.
- Si eres víctima, actúa rápido: cambia claves, informa al banco y denuncia.
- Habla con tus hijos de forma abierta, sin alarmarlos pero sí educándolos.

Capítulo 4: Control Parental y Protección de Menores

Introducción: ¿Por qué es importante hablar de esto?

Cada vez más niños y adolescentes utilizan móviles, tablets y ordenadores desde edades tempranas. Esto les abre un mundo de posibilidades educativas, sociales y de entretenimiento, pero también los expone a **riesgos** que los padres no siempre conocen: acceso a contenido inapropiado, ciberacoso, grooming (acercamiento con fines sexuales), exceso de pantalla, juegos con chats sin control, retos virales peligrosos...

Muchos padres dicen:

"No tengo idea de lo que hace mi hijo con el móvil."

"Sé que está en redes, pero no sé qué ve."

"No quiero invadir su privacidad, pero me preocupa."

Este capítulo busca ayudarte a encontrar el equilibrio: **ni vigilancia excesiva, ni desconexión total**. Hablamos de acompañamiento, no de espionaje.



¿Qué es el control parental?

El **control parental** se refiere a las herramientas y estrategias que los adultos utilizan para supervisar, limitar y guiar el uso que los menores hacen de la tecnología.

Incluye:

- **Filtrar contenidos** (pornografía, violencia, lenguaje inadecuado).
- **Limitar el tiempo de uso**.
- **Bloquear aplicaciones peligrosas** o no aptas.
- **Revisar actividad** en ciertas plataformas (sin leer conversaciones personales).

Pero el control parental **no sustituye la conversación y la educación**. De poco sirve bloquear un sitio si no se habla sobre por qué no es conveniente. Tampoco se trata de espiar, sino de acompañar.

El pilar básico: diálogo + tecnología

Antes de configurar apps o ajustes técnicos, es crucial hablar con tus hijos. Aquí algunas pautas para ese diálogo:

- **Empieza pronto:** Habla de esto antes de que surjan problemas. La prevención es más efectiva que la corrección.
- **Habla con respeto:** Evita tonos acusadores. Muestra interés genuino.
- **Escucha su opinión:** Pregunta qué hacen online, qué apps usan, qué les gusta. No todo lo digital es “malo”.
- **Acuerden reglas juntos:** Definan tiempos de uso, qué apps se pueden instalar, cómo actuar ante algo incómodo.
- **Da ejemplo:** Si tú estás todo el día con el móvil, el mensaje se contradice.

Recuerda: **el objetivo es enseñarles a cuidarse solos**. No estarán bajo tu control siempre, pero sí pueden estar bajo tu guía.

¿Dónde aplicar el control parental? Plataformas clave



Android y Google Family Link

Google ofrece una app gratuita llamada **Family Link**, muy útil para controlar el uso de móviles y tablets con Android. Permite:

- Establecer horarios de uso y tiempo por aplicación.
- Aprobar o bloquear nuevas apps.
- Ver cuánto tiempo pasan en cada app.
- Ubicar el dispositivo.
- Bloquear el móvil remotamente.



Consejo: Puedes instalarlo en tu móvil como padre/madre y vincular el de tus hijos fácilmente. Todo queda registrado en tu cuenta.



iPhone/iPad y Tiempo en Pantalla

Apple incluye **Tiempo en Pantalla**, una herramienta de control parental integrada. Permite:

- Limitar el tiempo de uso por día o app.
- Evitar compras sin permiso.
- Restringir contenido para adultos.
- Impedir cambios en los ajustes.
- Revisar el uso semanal.



Consejo: Establece un código (diferente al de desbloqueo) para evitar que lo desactiven.



Videojuegos y consolas

Las consolas como PlayStation, Xbox y Nintendo Switch tienen sus propios sistemas de control parental. Con ellos puedes:

- Limitar el tiempo de juego.
- Controlar con quién juegan online.
- Bloquear juegos no aptos para su edad.
- Recibir reportes semanales.



Consejo: En juegos populares como Fortnite, Roblox o Minecraft, también hay opciones de control dentro del juego. Investiga cada uno si tus hijos los usan.



YouTube y YouTube Kids

YouTube es una de las plataformas favoritas de los menores. Pero también una de las más delicadas.

- **YouTube Kids** es una versión filtrada. Recomendable para menores de 10 años.
- En **YouTube normal**, puedes activar el **modo restringido**, aunque no es infalible.
- Revisa el historial de búsqueda y visualización.
- Desactiva la reproducción automática.



Consejo: Crea listas de reproducción seguras tú mismo o junto a tus hijos.



Redes sociales (TikTok, Instagram, etc.)

Estas apps tienen millones de menores como usuarios, aunque algunas **requieren oficialmente 13 años para crear cuenta**. Aun así, muchos niños falsifican su edad para entrar.

TikTok tiene un modo "En Familia", que permite:

- Vincular tu cuenta con la del menor.
- Limitar el tiempo de uso.
- Desactivar mensajes privados.
- Filtrar contenido.



Consejo: Revisa la configuración de privacidad y seguridad de cada app. Asegúrate de que el perfil esté en modo privado.

Aplicaciones recomendadas para familias

1. **Qustodio** (Android/iOS) – Muy completa. Permite ver actividad, limitar apps, bloquear contenido y ver ubicación.
2. **Family Link** (Google) – Ideal para usuarios Android.
3. **Norton Family** – De los más completos para Windows.
4. **Microsoft Family Safety** – Para usuarios de PC, Xbox y móviles.
5. **KidLogger** – Para supervisar actividad en PC (registro de teclas, apps abiertas, etc.).

 Consejo: Algunas de estas apps son de pago, pero suelen ofrecer versiones gratuitas con funciones básicas.

Poner límites de pantalla sin conflictos (o con menos conflictos)

Poner límites no tiene que ser una batalla. Algunas ideas prácticas:

- **Usa el reloj, no la bronca:** “A las 19:00 se apaga el móvil” es mejor que “¡Llevas toda la tarde con el móvil, basta ya!”.
- **Horarios claros:** Define bloques del día sin pantallas (comidas, antes de dormir, deberes).
- **Pantallas visibles:** Nada de móvil en la habitación a puerta cerrada.
- **Alternativas atractivas:** Dejar el móvil duele menos si hay otra cosa que hacer: salir, cocinar, leer, jugar a algo.
- **Premia el buen uso:** Si cumple los acuerdos, puedes flexibilizar los tiempos el fin de semana, por ejemplo.

¿Y los adolescentes? ¿Cómo proteger sin invadir?

Con los adolescentes, el control se vuelve más difícil y más delicado. Aquí el enfoque debe pasar de “controlar” a “negociar y acompañar”.

- Explícales que el control no es desconfianza, sino cuidado.
- Pídeles que te expliquen qué redes usan y por qué. Escucha sin juzgar.
- Llega a acuerdos, como revisar juntos la configuración de privacidad.
- Pregúntales si han visto algo que los haya incomodado. Normaliza hablar de lo que pasa en Internet.
- Cuéntales noticias reales de casos peligrosos. No para asustar, sino para sensibilizar.

Resumen del capítulo:

- El control parental no es solo una cuestión técnica, sino educativa.
- Existen herramientas muy útiles para configurar dispositivos, apps y plataformas de forma segura.
- Es vital acompañar con diálogo, acuerdos y ejemplo personal.
- Cada edad necesita un enfoque diferente.
- Más que prohibir, se trata de formar a los menores para que se cuiden incluso cuando no estemos.

Capítulo 5: Redes Sociales – Riesgos y Buenas Prácticas

Introducción: Las redes, una nueva plaza pública

Las redes sociales se han convertido en una parte fundamental de la vida digital de niños y adolescentes. Para ellos, son **espacios donde socializan, se expresan, aprenden, se divierten... y también se exponen**. Aunque muchas de estas plataformas están pensadas para mayores de 13 años, la realidad es que **cada vez más menores las usan desde edades tempranas**.

Esto plantea desafíos importantes para los padres:

- ¿Cómo guiar sin invadir?
- ¿Cómo proteger sin prohibir todo?
- ¿Qué riesgos reales hay?
- ¿Qué podemos hacer en casa?

Este capítulo busca dar respuesta a esas preguntas con ejemplos, recursos y estrategias prácticas.

¿Qué redes usan más los menores hoy?

Aunque esto cambia con el tiempo, en 2025 las redes más usadas por niños y adolescentes son:

Plataforma Edad mínima (oficial) ¿Por qué la usan?

TikTok	13 años	Videos cortos, virales, humor, música
Instagram	13 años	Fotos, historias, mensajes, imagen personal
YouTube	13 años (Kids desde 9)	Entretenimiento, aprendizaje, seguir creadores
Snapchat	13 años	Fotos que desaparecen, mensajería rápida
Twitch	13 años	Ver y comentar videojuegos en directo
WhatsApp	16 años (en Europa)	Comunicación directa, grupos escolares o sociales

La mayoría de estas plataformas permiten el contacto con **desconocidos**, tienen **contenido sin filtros estrictos** y están diseñadas para generar **uso prolongado o incluso adictivo**.

Principales riesgos de las redes sociales en menores



Exposición de datos personales

Los niños a menudo no entienden los peligros de publicar fotos, ubicación o datos personales. Un perfil público con fotos, nombre completo y ubicación puede facilitar el **acceso a personas malintencionadas**.

 Ciberacoso

Los insultos, exclusiones, burlas o difusión de fotos sin permiso ocurren con más frecuencia de la que se reconoce. El ciberacoso deja huellas emocionales profundas, especialmente cuando ocurre frente a una audiencia virtual.

 Grooming

El **grooming** es el proceso mediante el cual un adulto se gana la confianza de un menor online con el objetivo de obtener contenido íntimo o proponer encuentros reales. Comienza con una conversación aparentemente inocente.

 Adicción a la validación

Los "me gusta", visualizaciones y comentarios se convierten en una fuente de autoestima. Esto puede llevar a los menores a:

- Publicar contenido arriesgado para conseguir atención.
- Sentirse mal si no obtienen suficientes reacciones.
- Compararse constantemente con otros.

 Retos virales peligrosos

Cada cierto tiempo surgen desafíos en TikTok o Instagram que invitan a hacer cosas absurdas, peligrosas o degradantes. Algunos son simplemente cómicos, pero otros implican daños físicos o humillación.

 Desinformación y contenido inadecuado

Fakenews, teorías conspirativas, contenido sexual o violento pueden aparecer sin que el menor lo busque. Muchos algoritmos **no distinguen entre niño y adulto**.

¿Cómo afectan emocionalmente a tus hijos?

Las redes influyen en la **autoimagen**, en cómo gestionan la aceptación social y en su capacidad de atención. Algunos efectos observados en adolescentes con uso excesivo:

- **Ansiedad** por mantener una imagen perfecta.
- **Frustración** por no ser "tan populares" como otros.
- **Dependencia emocional** del móvil.
- **Aislamiento real**, pese a estar "conectados".

Por eso, no se trata solo de controlar tiempo de pantalla, sino de enseñarles a relacionarse sanamente con estas plataformas.

¿Qué pueden hacer los padres? Buenas prácticas

1. Ajustar la privacidad

- Asegúrate de que las cuentas estén **en modo privado**.
- Revisa la configuración de quién puede ver publicaciones, comentar o enviar mensajes.
- Desactiva la geolocalización en apps como Instagram o Snapchat.

2. Hablar del contenido que consumen y publican

- Pregunta qué cuentas siguen y por qué.
- Anima a reflexionar sobre lo que comparten: ¿Lo publicarías si tus abuelos lo vieran?
- Explícales que lo que se publica en Internet **nunca desaparece del todo**, incluso si lo borran.

3. Acuerdos claros sobre el uso

- Define horarios (por ejemplo, sin móvil durante las comidas o antes de dormir).
- Establece zonas sin tecnología en casa.
- Limita el tiempo en redes si afecta el sueño, el estudio o el ánimo.

4. Acompañar, no espiar

- Pide permiso para ver juntos sus perfiles si lo aceptan.
- Crea un entorno donde puedan hablar si ven algo raro sin miedo a castigos automáticos.
- Si decides usar herramientas de supervisión, explícaselo y hazlo con transparencia.

Ideas para conversar en casa

- "¿Has visto algo en redes que te haya hecho sentir incómodo/a últimamente?"
- "¿Qué opinas de las fotos que ves en Instagram? ¿Te parece que reflejan la realidad?"
- "¿Tú qué harías si alguien que no conoces te habla por mensaje privado?"
- "¿Crees que hay presión por mostrar solo lo bueno o lo bonito en las redes?"

Estas conversaciones ayudan a que los menores **desarrollen criterio propio** y te vean como un aliado, no como un policía.

¿Y si ya ha pasado algo? ¿Qué hacer?

- Escucha sin juzgar. Lo más importante es que tu hijo confíe en que puede hablar contigo.
- Guarda capturas de pantalla como prueba.
- Denuncia contenido abusivo directamente en la plataforma.
- Si hay acoso, grooming o amenazas, contacta con la policía o la Unidad de Delitos Telemáticos.

Recursos útiles

- PantallasAmigas.net: educación y prevención en el uso seguro de Internet.
- INCIBE – Internet Segura for Kids (IS4K): portal oficial con guías, vídeos y asesoramiento gratuito.
- OSI – Oficina de Seguridad del Internauta: alertas, consejos y cómo actuar en casos de fraude.

- Common Sense Media: reseñas sobre apps, juegos y películas adaptadas por edades (en inglés, pero muy completo).

Resumen del capítulo:

- Las redes sociales son parte integral de la vida juvenil, pero requieren acompañamiento.
- Los riesgos incluyen exposición, ciberacoso, grooming, adicción y desinformación.
- Ajustar configuraciones de privacidad es necesario pero no suficiente.
- El diálogo constante, los acuerdos familiares y el ejemplo adulto son la mejor defensa.
- Si surge un problema, actuar con calma y apoyo es clave para proteger emocionalmente al menor.

Capítulo 6: Seguridad en Dispositivos y Redes del Hogar

Introducción: ¿Por qué proteger también la casa?

Hoy en día, tu hogar no solo tiene puertas y ventanas que proteger: **también tiene una red Wi-Fi, dispositivos conectados y accesos digitales**. Un fallo de seguridad doméstico puede exponer tu información personal, dejar abierta la puerta a ataques y comprometer incluso los móviles o tablets de tus hijos.

Muchos padres se preocupan por lo que pasa “fuera” en Internet, pero no saben que **la primera línea de defensa está dentro de casa**: el router, los dispositivos, los hábitos digitales cotidianos.

En este capítulo aprenderás cómo blindar digitalmente tu hogar con pasos sencillos pero potentes.

Parte 1: Protegiendo la red Wi-Fi del hogar

La red Wi-Fi es el **punto por el que todos los dispositivos se conectan a Internet**. Si esa red es débil o está mal configurada, cualquier persona con malas intenciones podría:

- Interceptar tus datos.
- Usar tu conexión para actividades ilegales.
- Entrar a dispositivos conectados en casa (como cámaras, televisores o móviles).



7 pasos clave para una red Wi-Fi segura

1. Cambia la contraseña predeterminada del router

- Nunca dejes la contraseña que viene de fábrica (a veces es “admin” o “1234”).
- Usa una contraseña robusta: más de 10 caracteres, con letras, números y símbolos.

2. Cambia el nombre de la red (SSID)

- No uses nombres como “Casa de Luis” o “WiFi Pérez”. Es mejor algo neutro, como “RedPrivada38”.

3. Activa el cifrado WPA3 (o WPA2 al menos)

- Ve a los ajustes del router y asegúrate de que el cifrado está en “WPA2” o “WPA3”.
- Evita redes “abiertas” o sin contraseña.

4. Oculta el SSID (opcional)

- Puedes configurar el router para que no anuncie el nombre de la red. Así, solo quien lo sepa podrá conectarse.

5. Desactiva WPS

- Es una función que permite conectarse apretando un botón físico del router, pero puede ser insegura.

6. Actualiza el firmware del router

- Los routers tienen un “sistema operativo” que debe mantenerse al día. Entra a la interfaz del router y busca actualizaciones.

7. No compartas tu Wi-Fi sin cuidado

- Si vienen visitas, es mejor crear una red de invitados, separada de la red principal.



Parte 2: Seguridad en móviles, tablets y ordenadores

Cada dispositivo conectado a la red es un **posible punto de entrada**. Aquí te muestro cómo blindarlos de forma sencilla.

Móviles y tablets

- **Mantén el sistema operativo actualizado** (Android o iOS). Las actualizaciones corrigen fallos de seguridad.
- **Activa el bloqueo con PIN, huella o rostro.**
- **Instala solo apps desde tiendas oficiales (Google Play, App Store).**
- **Revisa los permisos que das a cada app:** ¿una linterna necesita acceso a tus fotos? Probablemente no.
- **Evita el “root” o “jailbreak”,** que desprotegen el sistema.
- **No uses redes Wi-Fi públicas sin protección.** Si es inevitable, mejor navegar con una VPN.

Ordenadores (Windows o Mac)

- **Instala antivirus confiable.** Ejemplos: Bitdefender, Avast, Kaspersky, Norton.
- **Activa el cortafuegos del sistema.**
- **Actualiza el sistema operativo y los programas regularmente.**
- **Evita abrir archivos o correos de fuentes desconocidas.**
- **No dejes sesiones abiertas en sitios web sensibles.**
- **Usa navegadores actualizados y extensiones de seguridad si es necesario.**

Parte 3: Dispositivos inteligentes (Smart Home)

Cada vez hay más objetos del hogar conectados a Internet: televisores, altavoces, cámaras de seguridad, asistentes de voz, incluso frigoríficos. Estos dispositivos pueden ser útiles... **pero también peligrosos si no están bien configurados.**



Riesgos comunes:

- Pueden ser espiados o controlados desde fuera.
- Si tienen cámaras, pueden grabar sin tu conocimiento.
- Si están desactualizados, pueden ser usados por ciberdelincuentes como “puertas traseras”.



Consejos prácticos:

1. **Cambia las contraseñas de fábrica de todos los dispositivos.**
2. **Actualiza el firmware del dispositivo desde su app oficial.**
3. **Desactiva funciones que no uses (como el micrófono o la cámara).**
4. **No pongas dispositivos “inteligentes” en habitaciones privadas.**
5. **Usa una red Wi-Fi separada solo para domótica si tu router lo permite.**

Parte 4: Buenas prácticas familiares

La seguridad digital no depende solo de la tecnología, sino de **los hábitos diarios**. Aquí van unas normas básicas para toda la familia:



Para hijos:

- No descargar apps sin pedir permiso.
- Avisar si el dispositivo se comporta raro (se apaga solo, aparecen ventanas nuevas, etc.).
- No uses cargadores públicos sin consultar.
- No conectarse a redes Wi-Fi abiertas sin hablarlo contigo.



Para adultos:

- Revisar periódicamente los dispositivos del hogar.
- Tener una lista de los dispositivos conectados al Wi-Fi (se puede ver desde la app del router).
- Establecer horarios de uso del Internet (por ejemplo, desconectarlo por la noche si nadie lo usa).
- Educar con el ejemplo: tú también debes cuidar tus contraseñas y hábitos online.

Parte 5: ¿Cómo saber si algo va mal?

Aquí algunas señales de alerta:

- La conexión Wi-Fi se vuelve lenta sin razón.
- El router se reinicia solo.
- Aparecen apps o iconos nuevos que nadie ha instalado.
- Se reciben mensajes de confirmación de inicio de sesión que no has hecho.
- La cámara o el micrófono se activan sin permiso.

¿Qué hacer?

- **Cambiar contraseñas inmediatamente.**
- **Reiniciar el router y revisar dispositivos conectados.**
- **Actualizar todo el software posible.**
- **Consultar con un técnico o con la Oficina de Seguridad del Internauta (OSI).**

Recursos útiles:

- <https://www.osi.es>: Guías de seguridad para dispositivos y Wi-Fi.
- <https://www.incibe.es>: Ciberseguridad para ciudadanos.
- <https://haveibeenpwned.com>: Comprueba si tu email o contraseña han sido filtrados.

Resumen del capítulo:

- Tu red Wi-Fi es la entrada a tu casa digital: protégela como la puerta de entrada.
- Todos los dispositivos deben estar configurados con seguridad básica.
- Los altavoces, cámaras y Smart TVs también pueden ser vulnerables.
- Los hábitos de seguridad valen tanto o más que las herramientas.
- Revisar, actualizar y hablar en familia es clave para tener un hogar digital protegido.

Capítulo 7: Herramientas Útiles para Padres Digitales

Introducción: No necesitas ser experto, solo estar bien acompañado

Muchos padres se sienten sobrepasados por la tecnología. Pero la buena noticia es que **no hace falta ser ingeniero informático** para proteger y educar digitalmente a tus hijos. Existen herramientas pensadas específicamente para ti: fáciles, efectivas y muchas veces gratuitas.

Este capítulo recopila las más útiles para acompañar a tus hijos con seguridad y criterio. Están divididas por categorías: control parental, buscadores, navegadores, apps educativas y recursos para padres.

1. Aplicaciones de control parental

Estas apps permiten **supervisar el uso del móvil, limitar el tiempo en pantalla, bloquear contenidos y saber qué hacen tus hijos online.**



Qustodio

- Compatible con Android, iOS, Windows, Mac y Kindle.
- Funciones: tiempo de uso, bloqueo de apps, historial de actividad, geolocalización.
- Interfaz amigable para padres con poca experiencia.
- Versión gratuita limitada; versión premium con más funciones.

Ideal para: padres que quieren un panel completo de supervisión.



Google Family Link

- Gratis para Android y dispositivos con cuenta Google.
- Funciones: aprobación de apps, límite de tiempo, ubicación, estadísticas.
- Puedes ver el tiempo de pantalla diario y establecer horarios de descanso.

Ideal para: familias Android, especialmente con hijos menores de 13 años.



Norton Family

- Incluido en paquetes Norton de antivirus.
- Permite supervisar sitios visitados, controlar búsquedas, limitar tiempo.
- Buena integración con PC y dispositivos móviles.

Ideal para: familias que ya usan Norton o que buscan una solución integral.



Microsoft Family Safety

- Gratuita para usuarios de Windows, Xbox y móviles Android.
- Informes de actividad, límites de tiempo, bloqueo de contenidos web.

Ideal para: hogares con varios dispositivos Windows o Xbox.

Tabla comparativa rápida:

Herramienta	Compatible con	Gratis	Funciones destacadas
Qustodio	Android, iOS, PC	Limitada	Muy completa, interfaz sencilla
Family Link	Android, ChromeOS	Sí	Fácil de usar, buena para menores
Norton Family	Android, iOS, PC	No	Alta protección, requiere suscripción
Microsoft Family	Windows, Android	Sí	Buen complemento si usas Microsoft

2. Buscadores seguros para menores

Los buscadores tradicionales pueden mostrar contenido inapropiado incluso sin querer. Estos buscadores están diseñados para niños:

**Kiddle.co**

- Motor de búsqueda basado en Google, pero con filtros infantiles.
- Presenta resultados con lenguaje más simple y páginas moderadas.
- Diseño atractivo para niños.

**KidRex**

- Otro buscador filtrado con aspecto infantil.
- Filtra automáticamente contenido ofensivo.

**SafeSearch de Google**

- No es un buscador nuevo, pero puedes activarlo para bloquear imágenes explícitas.
- Se configura en la cuenta de Google.



Consejo: Aunque el filtro sea útil, sigue siendo importante acompañar la navegación.

3. Navegadores y sistemas operativos especiales**Zoodles (modo niños)**

- Crea un entorno cerrado para menores.
- Ideal para tablets de uso compartido en casa.
- Permite que los niños accedan solo a contenidos educativos y seguros.

**Kidoz**

- Navegador, reproductor de vídeos y centro de juegos seguro.
- Tiene control parental integrado.

Windows modo familiar

- Si usas Windows, puedes configurar el equipo en modo infantil con controles.

4. Extensiones útiles para el navegador

Pequeñas herramientas que puedes añadir a Google Chrome, Edge o Firefox para mejorar la seguridad.

- **BlockSite:** bloquea webs no deseadas.
- **StayFocusd:** limita el tiempo de navegación en ciertas páginas.
- **uBlock Origin:** bloquea anuncios peligrosos y rastreadores.
- **YouTube Kids (acceso directo):** filtra vídeos por edad.

 **Sugerencia:** Pide ayuda para instalar estas extensiones si nunca lo has hecho. O consulta tutoriales sencillos en YouTube.

5. Apps educativas para enseñar ciberseguridad a niños

Aprender a navegar seguros también es tarea de los niños. Estas apps y juegos lo hacen divertido:

Interland (de Google)

- Juego en línea donde los niños aprenden sobre privacidad, contraseñas y respeto digital.
- Gratuito y en español: <https://beinternetawesome.withgoogle.com>

Cyber Scouter

- App con retos interactivos que enseñan sobre phishing, contraseñas y redes sociales.

IS4K Juegos

- El portal Internet Segura for Kids tiene actividades por edades.
- Disponible en: <https://www.is4k.es>

6. Recursos para padres (aprender sin abrumarse)

Guías paso a paso

- **INCIBE** (Instituto Nacional de Ciberseguridad): Manuales claros sobre privacidad, grooming, acoso escolar y más. <https://www.incibe.es>
- **Pantallas Amigas:** Vídeos, infografías y campañas educativas. <https://www.pantallasamigas.net>
- **OSI (Oficina de Seguridad del Internauta):** Consejos de protección para adultos y familias. <https://www.osi.es>

7. ¿Cómo elegir la mejor herramienta para tu familia?

Pregúntate:

- ¿Qué edad tienen mis hijos?
- ¿Qué dispositivos usan más?
- ¿Cuánto tiempo puedo dedicar al seguimiento?
- ¿Prefiero una solución automática o acompañarlos directamente?

Si tienes poco tiempo, **elige 1 o 2 herramientas básicas** y empieza por ahí. Más vale poco y bien aplicado, que muchas apps sin seguimiento.

Resumen del capítulo:

- Existen muchas herramientas diseñadas para facilitar el papel de los padres digitales.
- No necesitas saber de informática: solo elegir lo que mejor se adapta a tu casa.
- El mejor filtro sigue siendo el acompañamiento humano, pero las herramientas ayudan.
- Explora, prueba, y elige lo que te dé tranquilidad y confianza para educar en el mundo digital.

Próximo capítulo:

En el **Capítulo 8: Cómo actuar ante un incidente (fraude, acoso, acceso no autorizado)** veremos qué pasos tomar si ocurre un problema real en casa o con tus hijos. Desde ataques por phishing, hasta el acoso escolar por redes.

Capítulo 8: Cómo actuar ante un incidente (fraude, acoso, acceso no autorizado)

Introducción: Cuando lo digital deja de ser seguro

Por muy buenas que sean las medidas de prevención, **los incidentes pueden ocurrir**. Un mensaje fraudulento, una cuenta hackeada, un hijo que sufre acoso digital o una aplicación que expone información privada. La clave no es solo prevenir, sino **saber cómo actuar con rapidez y eficacia**.

En este capítulo aprenderás:

- Cómo identificar señales de alerta.
- Qué pasos tomar según el tipo de incidente.
- Qué hacer emocionalmente si tu hijo ha sido víctima.
- Dónde denunciar o reportar problemas.
- Cómo reconstruir la seguridad tras el incidente.

Parte 1: Señales de que algo está mal

A veces los problemas no se ven al instante. Aquí algunas **señales comunes**:



En el dispositivo:

- El navegador se abre solo o redirige a webs raras.
- Aparecen apps que nadie instaló.
- El móvil o el PC va mucho más lento de repente.
- Saltan ventanas emergentes (pop-ups) sin motivo.
- El antivirus da avisos frecuentes.



En correos o mensajes:

- Correos sospechosos piden “verificar tu cuenta” con enlaces urgentes.
- Mensajes de redes sociales o WhatsApp con enlaces poco fiables (phishing).
- Peticiones de dinero o códigos por parte de contactos que “parecen” conocidos.



En tus hijos:

- Cambian de humor tras usar el móvil.
- Ocultan la pantalla si te acercas.
- Dejan de usar una red social de golpe.
- Se aíslan o muestran ansiedad repentina.
- Mencionan haber perdido acceso a una cuenta.

Parte 2: ¿Qué hacer ante un fraude (phishing, timo online)?

El phishing es uno de los fraudes más comunes. Puede llegar por correo, SMS, WhatsApp o redes sociales.

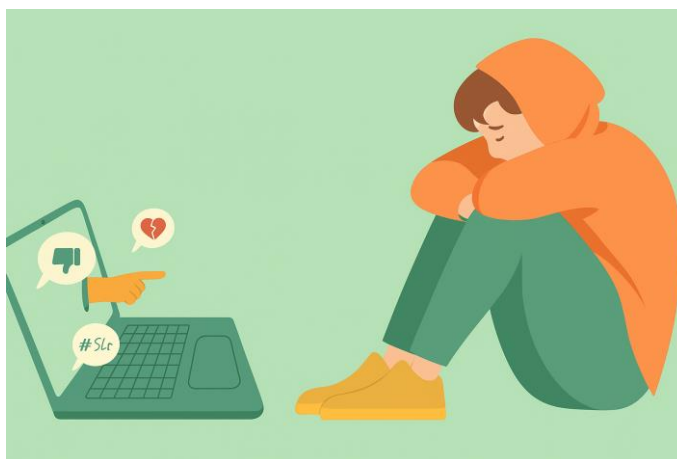
? ¿Qué hacer?

1. **No hagas clic en enlaces sospechosos.**
2. **No introduzcas datos personales ni bancarios.**
3. Si ya lo hiciste:
 - Cambia inmediatamente tus contraseñas.
 - Informa a tu banco si diste datos financieros.
 - Revisa tus movimientos bancarios recientes.



Revisa también:

- Si te piden verificar identidad, entra por tu cuenta (no desde el enlace del mensaje).
- Activa la **verificación en dos pasos** en tus cuentas más sensibles (bancos, email, redes).



Parte 3: ¿Qué hacer si tu hijo sufre ciberacoso?

El ciberacoso (o bullying digital) puede tener consecuencias emocionales graves. Es más frecuente en preadolescentes y adolescentes, y puede ocurrir por WhatsApp, Instagram, TikTok o incluso videojuegos.



Lo más importante: escucha sin juzgar.

Tu hijo necesita saber que no será castigado ni culpado por contarte lo que ocurre.

Pasos para actuar:

1. **Recoge pruebas:** haz capturas de pantalla del acoso.
2. **No respondas al acosador.**
3. **Bloquea al agresor en la plataforma.**
4. **Informa a la red social o app del incidente.**
5. Si el acoso continúa:
 - Contacta con el centro escolar.
 - Denuncia ante la policía si hay amenazas o se difunden imágenes privadas.

Parte 4: ¿Qué hacer si una cuenta ha sido hackeada?

Puede ocurrir con Instagram, Gmail, TikTok, incluso cuentas de videojuegos.



Pasos urgentes:

1. **Intenta recuperar el acceso con el correo electrónico de recuperación.**
2. **Cambia la contraseña inmediatamente.**
3. Si no puedes acceder:
 - Usa la opción “¿Olvidaste tu contraseña?”.
 - Contacta con el soporte oficial de la plataforma.
4. **Cambia también la contraseña en otras cuentas donde usabas la misma.**
5. **Activa la verificación en dos pasos** en todas las cuentas recuperadas.



Consejo:

Usa **un gestor de contraseñas** para crear claves seguras y diferentes. Ejemplos: Bitwarden, LastPass, 1Password.

Parte 5: ¿Qué hacer si tus datos fueron expuestos?

Si alguna app o sitio ha sido víctima de una filtración de datos (como contraseñas, correos, números de tarjeta), puedes comprobarlo.

Herramienta útil:

- <https://haveibeenpwned.com>: ingresa tu correo y sabrás si ha sido parte de una filtración conocida.

Qué hacer si aparece en la lista:

1. **Cambia inmediatamente la contraseña de esa cuenta.**
2. **Si usabas esa contraseña en otros sitios, cámbiala también.**
3. **Evita usar la misma contraseña en varias plataformas.**
4. **Habilita doble verificación (2FA).**

Parte 6: Cómo apoyar emocionalmente a tu hijo tras un incidente

Si tu hijo ha sido víctima de acoso, chantaje o pérdida de privacidad digital:



Qué necesita de ti:

- Escucha sin interrupciones.
- No le hagas sentir culpable por “haber caído”.
- Valida su experiencia: “Entiendo que estés asustado. Lo vamos a resolver.”
- Evita amenazas como “¡te quito el móvil para siempre!” (genera silencio y desconfianza).
- Refuerza que hizo lo correcto al contártelo.

Si hay impacto emocional fuerte, considera consultar con un profesional de la salud mental.

Parte 7: Dónde denunciar

Plataformas online:

- En casi todas las redes sociales puedes **reportar contenido** o perfiles abusivos directamente.



Policía:

- Puedes acudir a la policía nacional (presencialmente o por teléfono) si hay:
 - Amenazas.
 - Difusión de contenido íntimo.
 - Suplantación de identidad.
 - Casos de grooming.



Teléfonos útiles (España):

- **INCIBE ayuda (ciberacoso, sextorsión, dudas):** 017 (gratuito y confidencial).
- **Emergencias graves:** 112.

Parte 8: Reconstruir la seguridad tras el incidente

Después del susto, es importante recuperar la normalidad, pero también **aprender** del error:

- Haz un “chequeo general” de cuentas y dispositivos.
- Establece nuevas contraseñas seguras.
- Repasa con tu hijo lo que ocurrió y cómo prevenirlo.
- Habla en casa de forma abierta sobre la importancia de la ciberseguridad.
- Celebra que supiste actuar: todos aprendieron algo útil.

Resumen del capítulo

- Los incidentes digitales son reales y cada vez más frecuentes.
- Identificar señales tempranas puede evitar daños mayores.
- Hay pasos concretos que puedes seguir para recuperar cuentas, denunciar abusos o cortar fraudes.
- Tu actitud como madre o padre es clave para que tu hijo confíe en ti cuando algo va mal.
- La recuperación debe ser técnica y emocional.

Próximo capítulo:

En el **Capítulo 9: Hacia una cultura digital familiar**, hablaremos de cómo crear hábitos, valores y rutinas digitales en casa. No se trata solo de evitar lo malo, sino de cultivar lo bueno.

Capítulo 9: Hacia una cultura digital familiar

Introducción: No se trata solo de evitar lo malo, sino de construir lo bueno

Hasta ahora hemos hablado de riesgos, herramientas y prevención. Pero la ciberseguridad no es solo apagar fuegos: **también es sembrar buenos hábitos digitales en casa**, con propósito, valores y comunicación.

Este capítulo propone dar un paso más allá: **crear una cultura digital familiar**. No basta con controlar: hay que educar, acompañar, compartir y construir una relación sana con la tecnología como familia.

Parte 1: ¿Qué es una cultura digital familiar?

Una cultura digital familiar es el **conjunto de normas, actitudes, rutinas y valores compartidos** sobre cómo usamos la tecnología en casa. No nace sola: se construye con el ejemplo, el diálogo y la práctica cotidiana.



Señales de que hay una buena cultura digital en casa:

- Se habla abiertamente sobre lo que se hace online.
- Se respetan horarios y espacios sin pantallas.
- Padres e hijos colaboran en decisiones tecnológicas (ej: elegir apps, contenidos).
- Hay conciencia sobre privacidad, empatía digital y respeto.
- La tecnología se usa para aprender, divertirse y conectar (no solo para “matar el tiempo”).

Parte 2: Crear rutinas digitales saludables

Los hábitos no se imponen con miedo, se construyen con constancia. Aquí algunos pilares para estructurar una rutina digital sana:

1. Establecer horarios claros de uso

- Horarios para pantallas (por ejemplo: no móviles en la mesa, no tablets después de las 21:00).
- Alternar tiempo digital con tiempo sin tecnología (ej: leer en papel, juegos de mesa, deporte).
- Usar temporizadores si hace falta (ej: 30 minutos de TikTok, luego pausa).

2. Crear espacios sin pantallas

- Zonas “libres de pantallas” en casa: el comedor, las habitaciones, el baño.
- Poner cargadores en un lugar común fuera del dormitorio para dormir sin el móvil al lado.

3. Planificar pausas digitales

- Hacer descansos visuales y posturales: mirar al horizonte, estirarse, caminar.
- Introducir el concepto de “desconexión programada” (un día a la semana sin pantallas fuera del trabajo o estudios).

Parte 3: Valorar lo positivo del mundo digital

No todo en internet es peligro. La tecnología bien usada puede enriquecer muchísimo.

? ¿Cómo aprovechar lo bueno?

- Usar apps educativas juntos (juegos de palabras, historia, matemáticas).
- Ver documentales o canales de YouTube culturales como familia.
- Escuchar podcasts o audiolibros en grupo.
- Crear algo juntos: una presentación, un vídeo, una receta digital.
- Enseñar a investigar: buscar respuestas a curiosidades en familia.

La clave está en pasar de “consumir pantalla” a “crear con la pantalla”.

Parte 4: Establecer acuerdos familiares

Más allá de reglas, los acuerdos se construyen con todos los miembros de la casa.

? ¿Cómo hacerlo?

1. **Convoca una reunión digital familiar** (puede ser algo informal, una tarde con merienda).
2. Expongan los temas que preocupan a todos (tiempo en pantallas, juegos, privacidad).
3. Anoten juntos acuerdos simples, claros y visibles:
 - Ej: "No usamos móviles después de las 21:00".
 - Ej: "Si veo algo raro en internet, lo cuento sin miedo a ser castigado".
4. Peguen los acuerdos en un sitio visible (puerta del frigo, corcho de la entrada).
5. Revisen juntos cada mes si los acuerdos funcionan.

No hace falta que sean muchos. Lo importante es que **haya compromiso compartido**.

Parte 5: Liderar con el ejemplo

Los hijos imitan más lo que hacemos que lo que decimos.

? ¿Cómo ser un buen referente digital?

- No mires el móvil mientras hablas con ellos.
- Reconoce si pasas mucho tiempo en redes y cuéntales que también te cuesta.
- Comparte lo que te gusta aprender online (cursos, noticias, aficiones).
- Sé transparente con tus límites: “yo también tengo que dejar el móvil antes de dormir”.
- Celebra los logros digitales positivos (ej: tu hijo edita un vídeo, aprende algo nuevo).

Ser modelo no significa ser perfecto, sino **ser honesto y consciente**.

Parte 6: Una tecnología con sentido

Pregúntate: ¿qué tipo de relación quiero que mi hijo tenga con la tecnología?, ¿Una en la que sea dependiente, distraído y pasivo?, ¿O una donde la tecnología esté a su servicio, no al revés?

**Ideas para una tecnología con propósito:**

- Usar apps para organizarse (agendas, calendarios).
- Aprender programación básica o robótica como familia.
- Crear un blog de recetas, memorias o viajes familiares.
- Fomentar debates sobre lo que se ve online (“¿qué opinas de este vídeo?”).

Cuanto más significativa sea la relación con la tecnología, **menos espacio hay para el uso dañino o vacío.**

Parte 7: Adaptarse al cambio

Internet y las plataformas cambian todo el tiempo. Lo importante es que **la cultura familiar sea flexible.**

- Si aparece una red nueva, no la prohíbas sin conocerla: infórmate, pregúntale a tu hijo.
- Si una herramienta deja de funcionar, busca otra alternativa juntos.
- Lo más importante: que el vínculo de confianza permanezca, más allá del dispositivo.

Resumen del capítulo:

- Una buena cultura digital no se impone: se construye en casa, día a día.
- Crear rutinas, espacios y acuerdos ayuda a equilibrar el uso de pantallas.
- La tecnología puede ser un aliado educativo y creativo si se usa con intención.
- Liderar con el ejemplo es el mejor camino para educar con coherencia.
- La cultura digital familiar es la mejor vacuna a largo plazo contra los riesgos online.

Capítulo 10: Videojuegos, tiempo en pantalla y adicción digital

Introducción: ¿Diversión o preocupación?

Los videojuegos forman parte del día a día de muchos niños y adolescentes. Para algunos padres, son un misterio; para otros, una preocupación constante. Pero no todo es negativo: bien usados, los videojuegos pueden desarrollar habilidades, unir a la familia e incluso enseñar.

La clave está en entender **cuándo es sano y cuándo se vuelve un problema**. Este capítulo no busca demonizar los videojuegos, sino ofrecerte herramientas para gestionarlos con sentido común, límites y comunicación.

Parte 1: Qué aportan realmente los videojuegos

Aunque a menudo se presentan como una pérdida de tiempo, los videojuegos también tienen beneficios:



Beneficios cognitivos:

- Mejoran la **coordinación ojo-mano**.
- Estimulan la **resolución de problemas** y el pensamiento estratégico.
- Potencian la **creatividad**, sobre todo en juegos de construcción como Minecraft.



Beneficios emocionales:

- Ayudan a **manejar la frustración** (perder, volver a intentar).
- Dan sensación de **progreso y logro**.
- Son una vía de **desconexión y relajación**.



Beneficios sociales:

- En muchos casos, se juega en equipo o con amigos.
- Fomentan habilidades de **cooperación y comunicación**.
- Son un espacio donde los jóvenes se sienten “competentes” y reconocidos.

El problema surge cuando **el juego domina la vida**, desplaza otras actividades o genera conflicto familiar.

Parte 2: ¿Cuánto es demasiado?

No hay un número exacto universal, pero sí hay **señales claras** de uso excesivo:



Señales de alarma:

- Tu hijo se pone **agresivo o irritable** si no puede jugar.
- **Miente** sobre cuánto tiempo ha jugado.
- Descuidas otras responsabilidades (estudios, higiene, sueño).
- Se **aisla socialmente**, no quiere salir o participar en otras actividades.

- Solo se muestra motivado si se habla del juego.

En esos casos, no estamos hablando de ocio digital saludable, sino de **uso problemático** o incluso riesgo de **adicción conductual**.



Parte 3: Establecer límites sin generar guerra

Poner límites no tiene que convertirse en una batalla diaria. Aquí algunas estrategias:

1. Acuerdos de tiempo (no imposiciones)

- Negociar juntos cuánto tiempo es razonable cada día o semana.
- Dejar claro qué ocurre si no se respetan los tiempos.
- Usar herramientas como temporizadores o apps de control.

2. Prohibir no siempre funciona

- Prohibir por completo genera deseo y puede llevar al ocultamiento.
- Es más efectivo permitir un uso controlado y supervisado.
- Hablar sobre el contenido del juego también reduce el misterio.

3. Establecer “momentos sin pantallas”

- Comidas, estudio y antes de dormir deben ser espacios sin juego.
- Reforzar otras actividades atractivas: deporte, arte, lectura, tiempo libre.

4. Jugar juntos de vez en cuando

- Interesarte por el juego de tu hijo es una forma de conectar.
- Pregunta: “¿Qué te gusta de este juego?”, “¿Cuál es tu parte favorita?”
- Puedes descubrir que hay más profundidad de lo que imaginabas.

Parte 4: Elegir juegos adecuados

No todos los juegos son iguales. Existen etiquetas de edad y contenido que conviene conocer.

? ¿Qué es PEGI?

PEGI (Pan European Game Information) es el sistema de clasificación por edades para videojuegos en Europa.

Ejemplo:

- **PEGI 3:** apto para todas las edades.
- **PEGI 7:** puede incluir miedo leve o violencia muy moderada.
- **PEGI 12:** lenguaje malsonante leve o violencia no realista.
- **PEGI 16/18:** violencia explícita, drogas, apuestas.



Consejo: No solo mires la edad, **lee la descripción de contenido** (violencia, lenguaje, miedo, etc.).

También puedes usar sitios como:

- <https://www.pegi.info>
- <https://www.commonsensemedia.org>

Parte 5: Herramientas de control para videojuegos

Casi todas las consolas tienen opciones para padres.

Ejemplos:

- **Nintendo Switch:** App para móviles “Nintendo Switch Parental Controls”. Controlas tiempo, juegos, restricciones por edad.
- **PlayStation (Sony):** Configuración de usuario con límite de tiempo y gastos.
- **Xbox (Microsoft):** App “Xbox Family Settings”. Control de pantalla, actividad, chat.
- **PC / Steam:** Modo familiar (Steam Family View), bloqueo de contenidos.



Importante: Configurar estas herramientas **junto con tus hijos**, no como castigo oculto. Así comprenden el porqué.

Parte 6: ¿Y si ya hay adicción?

Si ves que tu hijo ha perdido el control sobre el juego, puede ser momento de buscar ayuda profesional.

Pasos recomendados:

1. No entres en pánico: el objetivo es **recuperar el equilibrio, no eliminar el juego**.
2. Habla sin culpar: “He notado que últimamente te cuesta dejar el juego, ¿te pasa algo?”
3. Establece reglas claras y realistas.
4. Considera apoyo psicológico si hay:
 - Aislamiento social.
 - Ansiedad cuando no juega.
 - Insomnio o alteración del humor.

5. Contacta con recursos como:

- Psicólogos especializados en adicción digital.
- Programas escolares o comunitarios sobre tecnología.

Parte 7: ¿Y si el juego puede ser una oportunidad?

No todos los videojuegos llevan al problema. Algunos pueden ser incluso una **salida profesional o educativa**.

- Programación de videojuegos.
- Diseño gráfico 3D.
- Creación de contenido (YouTube, Twitch) con sentido.
- Juegos que enseñan historia, ciencia o lógica.

Hablar de videojuegos **como parte de la cultura actual** es una forma de abrir puentes, no muros.

Resumen del capítulo:

- Los videojuegos pueden ser positivos si se usan con criterio.
- El exceso de juego puede esconder necesidades emocionales o sociales.
- Es clave acompañar, negociar, y establecer rutinas sanas.
- Las herramientas de control parental son útiles, pero no sustituyen al diálogo.
- Una buena relación con los videojuegos comienza con el ejemplo adulto.

Capítulo 11: Inteligencia artificial y niños: asistentes, apps y voz

Introducción: ¿Qué pasa cuando tus hijos le preguntan a una máquina?

La inteligencia artificial (IA) ya no es ciencia ficción. Está en nuestras casas, teléfonos, buscadores y asistentes de voz. Y, lo queramos o no, **los niños ya interactúan con IA casi a diario**, a veces sin saberlo. ¿Qué deben entender sobre esta tecnología? ¿Es segura? ¿Puede enseñar algo? ¿Qué límites debe haber?

Este capítulo ayuda a madres y padres a **guiar el uso de la IA con sentido crítico, educativo y seguro**, desde Alexa hasta ChatGPT.

Parte 1: ¿Qué es la inteligencia artificial? (Explicado sin tecnicismos)

La IA es una tecnología que **simula la forma en que las personas piensan, aprenden y responden**. No tiene conciencia, ni emociones, ni comprensión real, pero **es capaz de detectar patrones y ofrecer respuestas que “parecen humanas”**.

¿Cómo se manifiesta en casa?

- **Asistentes de voz:** Alexa, Siri, Google Assistant.
- **Chatbots:** como ChatGPT, que mantienen conversaciones.
- **Apps educativas o de juegos:** que adaptan preguntas al nivel del niño.
- **Plataformas de streaming:** que recomiendan vídeos según gustos.

Es importante que los niños **no crean que estas máquinas "lo saben todo"**. Son herramientas, no sabios.

Parte 2: Cómo usan la IA los niños

Los menores usan la IA en múltiples formas, a menudo de manera natural:

Asistentes de voz:

- Preguntan cosas (“¿cuánto es 7 por 9?”, “¿quién fue Picasso?”).
- Piden música o cuentos.
- A veces, **tratan al asistente como si fuera un adulto**.

Aplicaciones:

- Juegos que responden o aprenden del usuario.
- Apps que corrigen ejercicios o enseñan idiomas.
- Herramientas de dibujo, edición o historias interactivas.

Chatbots:

- Algunos usan versiones básicas de ChatGPT para estudiar o divertirse.

- Pueden hacer preguntas, inventar cuentos, resolver dudas.

Parte 3: Beneficios del uso bien guiado

La IA no es el enemigo. De hecho, bien usada, puede ser un **estímulo intelectual y creativo**.

Ventajas educativas:

- Fomenta la **curiosidad** y el deseo de aprender.
- Mejora el **vocabulario y la expresión**.
- Estimula el pensamiento lógico (“hazme una adivinanza” o “explícame esto como si tuviera 5 años”).

Ventajas creativas:

- Inventar cuentos juntos (ChatGPT).
- Hacer dibujos con IA (algunas apps permiten crear arte digital).
- Crear canciones o poemas personalizados.

Ventajas comunicativas:

- Practicar idiomas con IA (inglés, francés...).
- Ejercitar el “pensar en voz alta” al conversar con asistentes.

Parte 4: Riesgos si no hay supervisión

Aunque no sean peligrosas en sí mismas, las IAs **no siempre dan respuestas adecuadas o completas**. Y los niños no siempre distinguen entre **información, opinión o error**.

Riesgos principales:

- **Desinformación:** IA puede inventar datos si no sabe la respuesta.
- **Confusión emocional:** algunos niños pueden “encariñarse” con el asistente.
- **Dependencia:** si el niño consulta todo a una IA, puede dejar de pensar por sí mismo.
- **Contenido inadecuado:** algunas IA pueden dar respuestas no aptas para ciertas edades si no se configuran bien.

Solución:

- Usar IA **acompañados por un adulto**, al menos al principio.
- Enseñarles que **no todo lo que dice una IA es cierto**.
- Preguntar: “¿Cómo podríamos comprobar si esto es verdad?”

Parte 5: Cómo enseñar pensamiento crítico con IA

No se trata de evitar que usen IA, sino de **ayudarles a usarla bien**.



Ideas prácticas:

1. Comparar fuentes:

- “Alexa dijo esto... ¿qué dice Google? ¿Qué dice un libro?”

2. Jugar al “detective de errores”:

- Pedirle a ChatGPT algo y buscar fallos o imprecisiones juntos.

3. Inventar cuentos con moraleja:

- Pedir a la IA un cuento, luego discutir juntos qué enseña y si tiene sentido.

4. Aprender a formular buenas preguntas:

- Ayudarles a hacer preguntas claras, completas y respetuosas.

Así enseñamos a que no usen la IA pasivamente, sino **como herramienta activa de aprendizaje**.

Parte 6: Actividades divertidas y educativas con IA

Aquí algunas ideas para experimentar en familia:



1. Crear un cuento personalizado

- Pedir: “Inventa un cuento corto con mi hijo Marcos como protagonista y un dragón que da consejos de salud”.



2. Generar imágenes

- Con apps como DALL-E o Bing Image Creator (si el niño es mayor y con supervisión), crear imágenes de “un robot tocando la guitarra en la Luna”.



3. Jugar a adivinar

- “Hazme una adivinanza difícil” y resolverla en familia.



4. Repasar para el cole

- “Explicame la fotosíntesis de forma sencilla”.
- “Hazme un test de 5 preguntas sobre los planetas”.

Parte 7: Normas para un uso seguro

Como con todo, lo ideal es combinar libertad con responsabilidad:

Reglas recomendadas:

- La IA no sustituye al profesor, ni al padre/madre.
- Si no entiendes algo que dice, pregunta.
- Nunca compartas tu nombre completo, dirección ni datos personales con un chatbot.

- Usar la IA solo en zonas comunes, no a solas y sin supervisión.
- Limitar el tiempo de uso como cualquier otra pantalla.

Parte 8: ¿Qué viene en el futuro?

La IA formará parte de la vida laboral y educativa de tus hijos. Lo importante es **que no la vean como magia ni como amenaza**, sino como una herramienta poderosa que deben saber manejar.



Reflexión final:

Enseñar a nuestros hijos a convivir con la IA es como enseñarles a conducir: **no basta con subirlos al coche, hay que enseñarles el volante, el freno y las señales.**

Resumen del capítulo:

- La IA ya convive con nuestros hijos, a menudo sin que lo sepamos.
- Bien usada, puede ser educativa, creativa y divertida.
- Es clave enseñarles a pensar críticamente, no solo a preguntar.
- La supervisión adulta sigue siendo imprescindible.
- Más que temer a la IA, hay que **preparar a los niños para entenderla, usarla y mejorarla.**

Capítulo 12: Privacidad de los padres: lo que también debemos proteger

Introducción: Tus datos también son el ejemplo

Cuando hablamos de ciberseguridad y menores, solemos centrarnos en los riesgos que enfrentan los hijos. Pero hay algo igual de importante: **la privacidad de los adultos también está en juego**. Y lo que los padres comparten, publican o descuidan en Internet **educa por imitación**.



Este capítulo aborda cómo proteger tus propios datos digitales —porque hacerlo **es parte de criar en el mundo conectado**.

Parte 1: ¿Qué es tu "huella digital"?

Cada vez que creas una cuenta, subes una foto o das tu correo para un sorteo, **estás dejando una huella digital**. Esa huella incluye:

- Tu nombre completo
- Tus redes sociales
- Tus gustos, ubicaciones y opiniones
- Imágenes familiares
- Datos financieros, incluso sin darte cuenta

Tus hijos observan cómo te manejas online. Si tú das demasiada información sin filtro, probablemente ellos lo harán también.

Parte 2: Riesgos más comunes para adultos online

Aunque a veces pensemos que “eso le pasa a otros”, estos riesgos son reales y frecuentes:

Suplantación de identidad:

- Alguien crea una cuenta falsa con tus datos o fotos.
- Puede estafar a tus contactos en tu nombre.

Phishing y estafas:

- Correos o mensajes falsos que te piden claves, pin, tarjetas.
- Simulan ser bancos, Amazon, Correos, la Seguridad Social, etc.

Exposición de imágenes familiares:

- Fotos de niños o de tu hogar pueden ser reutilizadas sin permiso.
- Algunos adultos suben fotos escolares, médicas, del parque, sin pensar en el contexto.

Contraseñas débiles o repetidas:

- Usar "123456" o "tuapellido2024" en todos los sitios es una invitación al desastre.

Parte 3: Buenas prácticas digitales para padres **1. Usa contraseñas seguras y únicas**

- Crea frases largas que puedas recordar. Ejemplo: "ElPerroDeMiVecina1998"
- No uses la misma contraseña en varios sitios.
- Activa la verificación en dos pasos (2FA) donde puedas.

 2. Ten cuidado con lo que publicas

- Evita mostrar:
 - Placas de colegio.
 - Ropa con nombres.
 - Lugares habituales (parque, casa, ruta diaria).
- Si subes fotos familiares, piensa: **¿le molestaría a mi hijo verlo dentro de 5 años?**

 3. Configura bien tus redes sociales

- Facebook: revisa quién puede ver tus publicaciones. Activa alertas de inicio de sesión.
- Instagram: mejor perfil privado si compartes familia.
- WhatsApp: puedes ocultar tu foto y última conexión a personas no guardadas.
- TikTok: si lo usas, asegúrate de que los videos familiares no estén públicos.

 4. Cuidado con sorteos y tests virales

- "¿Qué personaje de Disney eres?" puede parecer inofensivo, pero recolectan datos.
- No ingreses tu email o teléfono en sitios dudosos.

Parte 4: Tu correo y tus dispositivos también importan **El correo electrónico**

- Evita abrir correos de remitentes desconocidos con enlaces o archivos.

- Cuidado con mensajes tipo: “Tu paquete está retenido” o “verifica tu cuenta bancaria”.
- Ten al menos dos correos: uno personal y otro para registros de apps/suscripciones.



El móvil y el ordenador

- Usa antivirus si es posible.
- Mantén el sistema operativo actualizado.
- Activa el bloqueo de pantalla (PIN, huella o patrón).
- No prestes tu dispositivo desbloqueado a desconocidos.

Parte 5: Lo que compartes sobre tus hijos también es tu privacidad

A esto se le llama **sharenting**: compartir constantemente imágenes o detalles de tus hijos sin pensar en su intimidad futura.

Reglas sencillas:

- No publiques fotos de tu hijo desnudo o en ropa interior, ni siquiera si “es tierna”.
- No hagas públicas peleas familiares o problemas personales.
- Si tu hijo ya tiene edad para opinar (aunque sea 6 años), pregúntale antes: “¿Te importa si subo esta foto?”

Recuerda: **lo que hoy parece inofensivo puede tener consecuencias en la adolescencia.**

Parte 6: Liderar con el ejemplo

Tus hijos verán cómo gestionas tus dispositivos, cómo reaccionas a los mensajes sospechosos, o si te expones demasiado online.

Ideas concretas:

- Comenta en voz alta cuando detectas un correo sospechoso: “Esto no lo voy a abrir, parece falso”.
- Si alguien te pide tus datos por teléfono o mensaje, diles a tus hijos: “Nunca doy información sin verificar”.
- Cuando publiques algo en redes, comenta: “Voy a ocultar la ubicación por seguridad”.

Esto no es exagerar. Es **formar conciencia digital** en casa.

Parte 7: ¿Y si ya hubo un incidente?

Si sientes que has caído en una estafa o que tu privacidad fue vulnerada:

1. **Cambia contraseñas** de inmediato.
2. **Contacta con el banco** si diste datos financieros.
3. **Denuncia en la Policía** si usaron tu imagen o suplantaron tu identidad.

4. **Informa a tus contactos** si crees que pueden recibir mensajes falsos en tu nombre.

Resumen del capítulo:

- La privacidad digital no es solo para menores: también protege a los padres.
- Lo que tú haces online enseña (más que lo que tú dices).
- Usa herramientas, configura redes y publica con criterio.
- Cuidar tu privacidad **es parte de cuidar a tu familia.**

Capítulo 13: Herramientas para educar digitalmente en el aula y en casa

Introducción: tecnología para aprender, no para distraer

La educación digital no es el futuro: **es el presente**. Desde el colegio hasta el salón de casa, existen hoy decenas de herramientas que permiten reforzar el aprendizaje, despertar la curiosidad o incluso descubrir nuevas vocaciones en los más jóvenes.

Este capítulo está pensado para padres y docentes que quieren **acompañar el aprendizaje con tecnología, sin perderse ni depender de ella**. Ni hay que ser experto, ni hay que tener lo último: basta con saber **qué usar, cómo y para qué**.

Parte 1: Plataformas educativas fiables y gratuitas

Estas plataformas han demostrado su utilidad y calidad. Son seguras, accesibles y tienen contenidos para primaria, secundaria y más.



Khan Academy

- <https://www.khanacademy.org>
- Ideal para matemáticas, ciencias, historia y programación.
- Con vídeos, ejercicios interactivos y seguimiento de progreso.
- Disponible en español. Gratuita.



Duolingo

- <https://www.duolingo.com>
- Para aprender idiomas (inglés, francés, alemán, etc.).
- Juegos, premios y lecciones breves.
- Muy fácil de usar, incluso para niños desde 6 años.



Code.org

- <https://code.org>
- Enseña pensamiento computacional y programación de forma lúdica.
- Se puede empezar sin saber nada de código.
- Excelente para desarrollar lógica y creatividad.



Genially

- <https://www.genial.ly>
- Herramienta para crear presentaciones interactivas, mapas mentales, juegos y cómics educativos.

- Muy visual, atractiva para trabajar contenidos escolares o familiares.

Parte 2: Aplicaciones útiles por materia

Aquí algunas apps (gratuitas o con partes gratuitas) que pueden reforzar asignaturas específicas:



Matemáticas:

- **Photomath:** escanea problemas y muestra cómo resolverlos paso a paso.
- **Khan Academy Kids (para los más pequeños).**
- **Smartick:** ejercicios de cálculo adaptados al nivel del niño.



Lectura y comprensión:

- **Storyberries:** cuentos gratuitos online en varios idiomas.
- **Libro Móvil:** biblioteca gratuita para descargar y leer sin conexión.
- **Tales with GiGi:** cuentos animados leídos en voz alta.



Idiomas:

- **Duolingo, Lingokids (versión infantil), LyricsTraining (aprender con canciones).**



Pensamiento lógico:

- **Lightbot:** juego para aprender programación.
- **Thinkrolls:** puzzles de física y lógica para primaria.
- **ScratchJr y Scratch:** para crear historias y juegos (muy visual).

Parte 3: YouTube también puede enseñar (si sabes cómo)

Aunque muchos lo usan para entretenimiento, **YouTube puede ser una gran fuente de aprendizaje**, si se usa con criterio y control.



Cómo aprovecharlo:

- Activa el **modo restringido** para bloquear contenidos inapropiados.
- Supervisa qué canales siguen los niños.
- Usa **listas de reproducción** con vídeos que apoyen tareas escolares o intereses personales.



Canales educativos recomendados:

- **Happy Learning Español:** vídeos de ciencias, historia, medio ambiente.
- **Academia Play:** contenido para adolescentes con estilo visual dinámico.
- **QuantumFracture:** física explicada con animaciones.
- **Smile and Learn:** para niños pequeños, en español.

Parte 4: Crear es aprender: herramientas creativas

Además de consumir contenido, es fundamental que los niños **creen el suyo**. Estas herramientas son perfectas para hacerlo:

Hacer cómics o cuentos:

- **Pixton**: crea cómics con personajes y escenarios personalizables.
- **StoryJumper**: para escribir cuentos y exportarlos en PDF.
- **Canva**: plantillas para pósters, cuentos, infografías.

Crear juegos:

- **Scratch (desde 8 años)**: programar juegos sencillos sin código.
- **Bloxels**: diseñar videojuegos visuales.

Crear presentaciones o mapas mentales:

- **Genially**: para presentaciones interactivas.
- **MindMeister** o **Miro**: mapas mentales colaborativos.

Parte 5: Cómo acompañar el aprendizaje digital sin sobrecontrolar

La tecnología debe unir y enriquecer. **No se trata de controlar como un vigilante**, sino de estar presente, orientar y dar libertad con marco.

Estrategias para padres:

- **Pregunta con interés**: “¿Qué estás aprendiendo en esa app?” en lugar de “¿Qué haces pegado a esa pantalla?”
- **Hazlo juntos al principio**, luego deja que se autogestione.
- **Valida el esfuerzo**, no solo el resultado: “¡Veo que no te rindes!”, “¿Cómo hiciste eso?”

Para docentes:

- Usa estas herramientas **para reforzar, no reemplazar** contenidos.
- Recomienda recursos que puedan usar en casa.
- Fomenta que el alumno **explique lo que ha aprendido**, no solo que lo haga.

Parte 6: Actividades familiares con tecnología educativa

No hace falta una clase para aprender. Aquí algunas ideas para aplicar en casa:

- Crear un cuento ilustrado familiar (StoryJumper o Canva).
- Grabar una presentación con voz sobre un tema escolar.
- Investigar juntos un país, su cultura e idioma.
- Hacer una cápsula del tiempo digital: un Genially con fotos, notas y dibujos de hoy.

La clave está en **usar la tecnología como medio, no como fin.**

Resumen del capítulo:

- Existen cientos de herramientas digitales que educan, motivan y conectan.
- Las plataformas deben elegirse por su contenido, no por su moda.
- Crear es tan importante como consumir: la educación digital es activa.
- Padres y docentes tienen un rol acompañante, no de policía.
- Aprender juntos, con criterio y curiosidad, es la mejor receta para esta era.

Capítulo 14: Cómo gestionar los conflictos digitales en casa

Introducción: si discutís por pantallas, no estáis solos

“¡Ya apaga eso!”

“Pero si solo llevo cinco minutos...”

“¡Te dije que lo dejes cuando termine la cena!”

“Es injusto...”

¿Te suena? **La tecnología no solo ha traído avances, también nuevos motivos de discusión familiar.** No es que la tecnología sea el problema, sino **cómo nos relacionamos con ella... y entre nosotros.**

Este capítulo no juzga ni da recetas mágicas. Busca ayudarte a **entender, anticipar y gestionar mejor los conflictos digitales**, y convertirlos, poco a poco, en oportunidades de aprendizaje familiar.



Parte 1: Por qué discutimos por pantallas

La tecnología despierta tensiones en casa por varias razones:



Tiempo de uso:

- ¿Cuánto es demasiado?
- ¿Antes o después de los deberes?
- ¿Qué pasa si dicen “es solo un rato más...” todos los días?



Contenido y tipo de uso:

- No es lo mismo leer que ver vídeos todo el día.
- Algunos padres aceptan juegos o redes, otros no.
- Hay miedo a lo que “puede pasar ahí dentro” (contactos, retos, adicción).



Dificultad para desconectar:

- Las pantallas estimulan, entretienen y retienen.
- A veces los niños **no pueden parar sin ayuda**, y eso frustra a todos.



Padres también estresados:

- Muchas veces, el problema no es la pantalla, sino **el cansancio, el trabajo, las preocupaciones**.
- En esas condiciones, un “¡Cinco minutos más!” puede ser la chispa de una pelea.

Parte 2: Cómo prevenir (la clave está antes del conflicto)

El secreto para discutir menos no es prohibir todo. Es tener **reglas, coherencia y diálogo previo**.



Estrategias preventivas:

1. Establecer horarios claros y visibles:

- “De lunes a viernes, 1 hora de pantalla después de los deberes.”
- “El sábado puedes jugar más, pero el domingo no después de las 19:00.”

2. Negociar con antelación:

- Hacer acuerdos por escrito si hace falta.
- A veces se cede, otras se exige. Pero lo importante es **evitar improvisar normas en caliente**.

3. Definir “pantallas útiles” vs. “pantallas recreativas”:

- YouTube para investigar una tarea no cuenta igual que TikTok sin rumbo.
- Esto ayuda a priorizar y equilibrar.

4. Dar alternativas atractivas:

- Si solo hay “no”, el niño volverá a la pantalla.
- Proponer juegos, salidas, hobbies reales.

5. Dar el ejemplo:

- Si tú cenas mirando el móvil, será difícil que acepten dejar el suyo.
- La coherencia educa más que las órdenes.

Parte 3: Cuando ya estalló la discusión

Hay veces en que, a pesar de todo, el conflicto ocurre. En ese momento, lo que más ayuda es **regular la emoción antes que imponer razón**.

**No hacer:**

- Gritar o castigar de forma impulsiva.
- Descalificar (“Eres un adicto”, “No haces nada bien”).
- Cortar el wifi como único método.

**Hacer:****1. Respira y retrasa la reacción:**

- “Ahora estamos muy molestos. Vamos a calmarnos y luego hablamos.”

2. Valida su emoción, aunque no su conducta:

- “Sé que te cuesta parar. A mí también me costaría si estuviera pasándolo bien.”

3. Redirige sin entrar en batalla:

- “No es negociable que ahora pares. Luego puedes contarme por qué estabas tan metido.”

4. Evita humillar o ridiculizar:

- Las frases tipo “Esto es una tontería” invalidan sus intereses y generan distancia.

Parte 4: Después del conflicto: transformar en aprendizaje

Una vez pasado el enojo, llega el momento clave: **hablar, entender y mejorar juntos**.

Pasos recomendados:

- **Conversar cuando ambos estén tranquilos.**
- **Escuchar su versión sin interrumpir.**
- **Pedir también que escuchen la tuya.**
- **Plantear cómo hacer las cosas mejor la próxima vez.**
- **Volver al acuerdo o, si hace falta, reformularlo.**

Este proceso fortalece el vínculo y enseña a resolver diferencias **sin gritar ni imponer**.

Parte 5: Casos reales y posibles soluciones**Caso 1: “Se pone agresivo cuando le quito el móvil”**

- Puede que necesite **preparación anticipada**: avisar 10 minutos antes.
- También ayuda ofrecer una alternativa o plan (cena, cuento, paseo).
- Si se repite, revisar juntos cuánto y cómo está usando ese dispositivo.

Caso 2: “Se esconde con el móvil en el baño”

- Habla sin acusar: “Me preocupa que uses el móvil a escondidas”.

- Refuerza la confianza: “No quiero controlarte, quiero ayudarte a usarlo bien”.
- Explora si hay vergüenza, adicción o simplemente deseo de intimidad.

Caso 3: “Dice que todos sus amigos tienen permiso menos él”

- No minimices. Eso duele de verdad.
- Escucha su punto, pero mantén tu criterio con argumentos: “Puede que otros lo usen más, pero yo te conozco y sé qué es mejor para ti.”
- Incluso puedes proponer: “¿Por qué no averiguamos qué hacen tus amigos y vemos si podemos encontrar un equilibrio?”

Parte 6: Cuidar el vínculo más allá de la tecnología

Al final del día, lo importante no es ganar una discusión por pantallas. Es **no perder el vínculo**.

Recomendaciones finales:

- Di más “te quiero” que “apaga eso”.
- Interésate por sus juegos o canales, aunque no los entiendas.
- Recuerda que detrás del uso de tecnología **hay un niño o adolescente que busca conexión, entretenimiento, evasión o reconocimiento**.

Educar con tecnología no es solo poner límites. Es **acompañar en la vida conectada, con presencia, cariño y firmeza**.

Resumen del capítulo:

- Es normal que haya conflictos por el uso de pantallas. No significa que estés educando mal.
- Lo importante es anticiparse, tener acuerdos claros y regular las emociones cuando ocurre el conflicto.
- Escuchar, validar y negociar después del enojo fortalece la relación familiar.
- Más que prohibir o ceder siempre, lo clave es **educar con equilibrio y ejemplo**.

Conclusión: Educar en el mundo digital también es amar con responsabilidad

La tecnología no ha llegado para sustituirnos como padres. Pero sí nos ha exigido **actualizarnos como guías**.

No importa si no creciste con internet, si nunca tuviste que enfrentarte a redes sociales, a videojuegos online o a mensajes desconocidos en la madrugada. Lo importante no es saberlo todo, sino **atreverse a aprender, preguntar, equivocarse... y volver a intentarlo**.

Este libro no pretende darte una fórmula perfecta, porque no existe. Cada familia es distinta, cada hijo o hija también. Lo que sí esperamos es haberte ofrecido **claridad, herramientas, calma y perspectiva** para acompañar este camino digital con más confianza.

Algunas ideas para llevar contigo:

- No necesitas controlar todo, pero **sí estar presente**.
- No se trata de prohibir por miedo, sino de **formar con criterio**.
- No siempre debes tener la última palabra, pero **sí el corazón abierto**.
- Si no sabes algo, dilo. **La honestidad también educa**.

Educar en ciberseguridad no es instalar un antivirus. Es **ayudar a nuestros hijos a vivir conectados sin perderse, a expresarse sin exponerse, a explorar sin ponerse en riesgo**.

Y para eso, también debemos cuidarnos a nosotros mismos: nuestra privacidad, nuestro lenguaje, nuestro tiempo frente a las pantallas. Porque los hijos no solo nos escuchan... **nos observan**.

Gracias por estar aquí

Si has llegado hasta este punto, enhorabuena. Has recorrido más de 60 páginas de reflexión, guía y acompañamiento.

Esperamos que esta lectura haya sido como una **conversación cercana con alguien que te entiende**. Que puedas volver a ella cuando lo necesites. Que la compartas con otros padres que quizá se sienten igual de perdidos o saturados.

Porque nadie nos enseñó a educar en la era digital. Pero juntos, aprendiendo paso a paso, **sí podemos hacerlo bien**.

El siguiente paso es tuyo

Quizá decidas revisar hoy tus redes. O hablar con tu hijo sobre lo que vio en YouTube. O cambiar una contraseña. O simplemente preguntar con curiosidad: “¿Qué estás haciendo en el móvil?”

Cada pequeño gesto cuenta. Cada conversación también.

Y en ese proceso, más que proteger dispositivos, estarás **protegiendo a las personas que más quieres.**

Gracias por confiar.

Gracias por cuidar.